HKIHRM SURVEY ON MONITORING AND PERSONAL DATA PRIVACY IN THE WORKPLACE

SURVEY FINDINGS

INTRODUCTION

The Data Protection Committee of Hong Kong Institute of Human Resource Management (HKIHRM), in co-operation with the Office of the Privacy Commissioner for Personal Data (PCO), during August and September 2004 conducted the Survey on “Monitoring and Personal Data Privacy in the Workplace”. The objectives of the survey were to get a better understanding of current policies and practices as regards workplace surveillance as adopted by companies in Hong Kong, and to raise corporate awareness of the need for compliance with the Personal Data (Privacy) Ordinance as regards workplace surveillance. In total, 86 companies responded to the Survey.

EXECUTIVE SUMMARY

Of the 86 companies surveyed, 84% of them have a policy on personal data privacy, including workplace surveillance or monitoring. These policies are in most cases communicated to employees (88%) and most of the communication is in written form (89%). Of those with no current policy, 64% indicated that they were considering instituting such a policy within one year. (*Sections 3 to 7*)

Regarding the policy on workplace monitoring, again 84% of surveyed companies adopt one or more types of monitoring. Over half the companies surveyed have installed applications to monitor the use of various electronic communication devices (e.g., Internet / intranet / email). The major reasons for this monitoring were cited as “prevention of improper behaviour", such as theft/vandalism and misuse of company resources. Some 60% of respondents indicated that they had a staff-card monitoring application in place for “security” purposes. (*Sections 8 and 9*)

The findings also indicated that the various types of monitoring are not implemented in an excessive manner. A major proportion of the companies surveyed indicated that they investigate or review information collected only when there is good reason to do so, such as in the case of investigating a harassment complaint. (*Section 12*)

Apart from monitoring various facilities within the workplace, almost all companies surveyed also adopted other measures, including training and open communication, to prevent the abuse of corporate electronic communication devices. (*Section 17*)

The findings indicated that training and open communication concerning monitoring and personal data policies have enhanced the effectiveness of various monitoring applications and also fostered better employee relations. (*Section 18*)

The Committee is of the opinion that while monitoring in the workplace is a legitimate requirement for security and other purposes, companies have the obligation to formulate appropriate monitoring policies and to strike a balance between corporate interests and the legitimate privacy rights of employees.

SURVEY COVERAGE

The coverage of this Survey includes:

- Application of monitoring facilities and method of communication [Section 8]
- Reasons for monitoring [Section 9]
- Who is being monitored [Section 10]
- Information collected/monitored and in what manner [Section 11]
- Condition under which information collected during monitoring is investigated/ reviewed [Section 12]
- How monitoring of electronic information/ electronic communications systems at workplace is executed [Section 13]
- Retention policy under workplace monitoring [Section 14]
- Retention period [Section 15]
- Trend in monitoring policies [Section 16]
- Precautions / alternatives for prevention of mis-use of electronic information/ electronic communications systems [Section 17]
- Opinions of workplace monitoring [Section 18]

SURVEY FINDINGS WITH TABLES

(A) PROFILES OF SURVEYED COMPANIES

(1) BUSINESS & SIZE

Over half of the companies surveyed (58% in total) are from the "Wholesale/ import/export/ trading/ distribution", "Business services/ professional services", "Financial services/ banking/ insurance" and "Transport/ services allied to transport" sectors. Two-thirds of the companies surveyed are large companies with over 100 employees.

% to total number of companies	Size of company				
Business Sector	<=100 employees	101 - 500 employees	501 - 1,000 employees	>=1,001 employees	**Total**
Wholesale/ import/export/ trading/ distribution	12%	7%	0%	0%	**19%**
Business services/ professional services	8%	3%	2%	1%	**15%**
Financial services/ banking/ insurance	2%	8%	1%	1%	**13%**
Transport/ services allied to transport (storage)	2%	5%	1%	3%	**12%**
Construction/ property development/ real estate	1%	1%	2%	3%	**8%**
Retail	2%	2%	1%	1%	**7%**
Community/ social/ personal services	0%	3%	2%	0%	**6%**
Electricity/ gas/ petrol	1%	1%	0%	2%	**5%**
Telecommunication	1%	1%	1%	0%	**3%**
Hotel	1%	1%	0%	0%	**2%**
Manufacturing	0%	0%	1%	1%	**2%**
Restaurant/ catering	1%	1%	0%	0%	**2%**
Others	0%	1%	0%	0%	**1%**
Conglomerates	0%	1%	1%	2%	**5%**
Total	**33%**	**37%**	**14%**	**16%**	**86**

(2) MANAGEMENT & SIZE

A slightly higher proportion of respondents was composed of local companies, or of multinational companies with their headquarters in Hong Kong (52%).

% to total number of companies	Size of company				
Company management	<=100 employees	101 - 500 employees	501 - 1,000 employees	>=1,001 employees	**Total**
Local company with majority of its business, operations and/ or head office in Hong Kong	10%	16%	8%	9%	**44%**
Multinational company with head office in Hong Kong and a world-wide/regional operation	1%	1%	2%	3%	**8%**
Multinational company with an overseas head office and a world-wide/regional operation	21%	20%	3%	3%	**48%**
Total	**33%**	**37%**	**14%**	**16%**	**86**

(B) PERSONAL DATA POLICIES IN THE WORKPLACE

(3) COMPANY WITH A PERSONAL DATA POLICY: AN OVERVIEW

A high proportion of the companies surveyed (84%) had a policy on personal data privacy. Among the few companies without a policy, most of them were considering to institute one within one year's time.

	% to total number of companies
Have a policy	**84%**
No policy	**16%**
- considering to have one in one year time	**10%**
- not plan to have one in near future	**6%**
Total number of companies	**86**

(4) WHO IS IN-CHARGE OF PERSONAL DATA POLICY

In most cases, the HR department is in charge of the personal data policy (74%). Among those companies that did not have a policy on personal data privacy, most of them (75%) had no idea of who was responsible for personal-data issues.

% to total number of companies	With a policy		Without a policy		
	In written document	Not in written form	Considered instituting one in 1 year's time	No plan to have one in the near future	**Total**
HR department	56%	8%	2%	0%	**66%**
HR & other department(s)	7%	0%	0%	1%	**8%**
Other department	7%	1%	1%	0%	**9%**
Regional/HQ overseas	5%	0%	0%	0%	**5%**
No response	0%	0%	7%	5%	**12%**
Total	**74%**	**9%**	**10%**	**6%**	**86**

(5) COMPANY WITH A PERSONAL DATA POLICY: BY MANAGEMENT AND SIZE OF COMPANY

Overall, a high proportion of surveyed companies (84%) had a policy on personal data privacy. Large companies and multinational companies are more likely to have one.

% of companies with a policy on personal data privacy (to total number of companies in the specific category)	Size of company				
Company management	<=100 employees	101 - 500 employees	501 - 1,000 employees	>=1,001 employees	**Total**
Local company with majority of its business, operations and/ or head office in Hong Kong	67%	86%	71%	100%	**82%**
Multinational company with head office in Hong Kong and a world-wide/regional operation	100%	100%	50%	100%	**86%**
Multinational company with an overseas head office and a world-wide/regional operation	83%	82%	100%	100%	**85%**
Total	**79%**	**84%**	**75%**	**100%**	**84%**

(6) EXTENT TO WHICH THE POLICY ON PERSONAL DATA PRIVACY IS COMMUNICATED TO EMPLOYEES

Of those companies with a policy, in most cases, the personal data privacy policy has been communicated to employees (88%) and is in written form (89%).

% to companies with a policy on personal data privacy	It is communicated to employees in general	It is not communicated to employees in general	**Total**
The policy is in written document	81%	8%	**89%**
The policy is not in written form	7%	4%	**11%**
Total	**88%**	**13%**	**72**

(7) WRITTEN GUIDELINES/ CODES OF PRACTICE ON RETRIEVING PERSONAL INFORMATION IN THE WORKPLACE

However, a lower proportion of companies (74%) has written guidelines/codes of practice on retrieving personal information in the workplace. This indicates that some companies among those with a written policy on personal data privacy, guidelines/ codes of practice on retrieving personal information at workplace are not covered.

% of companies having written guidelines/codes of practice on retrieving personal information in the workplace	Companies with personal data policies in the workplace		
	The policy is a written document	The policy is not in written form	**Total**
Yes	71%	3%	**74%**
No	17%	8%	**25%**
No response	1%	0%	**1%**
Total	**89%**	**11%**	**72**

(C) COMPANY MONITORING PRACTICES

(8) APPLICATION OF MONITORING FACILITIES AND METHOD OF COMMUNICATION

Over half the companies surveyed used a "Staff card" (60%), or applied monitoring facilities to the use of "internet" (57%), "intranet/ server/ computer files" (55%) and "email" (56%). The use of most of the monitoring facilities is communicated to staff (over 80% of companies), but less than 70% of companies have a written document in this regard, and communications about monitoring of "Phone calls" and "CCTV/video" are less likely to be in written-document form to which employees can refer.

% to companies using monitoring facilities in specific area	**% of companies having monitoring facilities applied**	Monitoring practices are communicated to employees	Method of communication			**Number of companies using monitoring facilities in the area**
			With a written document that employees can refer to	Verbally communicated only	Others	
Internet	**57%**	80%	59%	18%	4%	**49**
Intranet/ server/ computer files	**55%**	81%	55%	23%	2%	**47**
Email	**56%**	88%	69%	17%	2%	**48**
Phone call	**29%**	92%	48%	40%	4%	**25**
CCTV/Video	**43%**	83%	39%	43%	3%	**37**
Staff card	**60%**	90%	61%	29%	4%	**52**
Others (fingerprint electronic record, Handkey system)	**2%**	100%	100%	0%	0%	**2**
Total number of companies	**86**					

(9) REASONS FOR MONITORING

"Monitoring improper behaviour" and "Security" are the most commonly cited reasons for monitoring, except for "Phone call" monitoring. While "As potential evidence for legal liability", "Collecting evidence for investigation" and "Protection of trade secrets/ proprietary information" are cited less often, they are usually some of the reasons for monitoring the use of electronic devices (internet, intranet and email). "Productivity monitoring" is the least cited reason, and is a relatively common reason for "Phone call" and "Staff card" monitoring.

% to companies using monitoring facilities in specific area	Reason(s) of monitoring							**Number of companies using monitoring facilities in the area**
	Productivity monitoring	Monitoring improper behaviour (e.g., theft/ vandalism/ misuse of company resources)	As potential evidence for legal liability	Collecting evidence for investigation (e.g., misconduct or harassment investigation)	Protection of trade secrets/ proprietary information	Security	Others	
Internet	20%	**69%**	18%	20%	33%	**55%**	2%	**49**
Intranet/ server/ computer files	15%	**57%**	19%	19%	47%	**55%**	4%	**47**
Email	23%	**67%**	27%	33%	38%	48%	6%	**48**
Phone call	**44%**	**36%**	32%	**36%**	16%	12%	20%	**25**
CCTV/Video	5%	46%	22%	24%	8%	**86%**	3%	**37**
Staff card	40%	21%	12%	10%	6%	**75%**	10%	**52**
Others (fingerprint electronic record, Handkey system)	50%	50%	50%	0%	0%	**100%**	50%	**2**

(10) WHO IS BEING MONITORED

Most of the monitoring facilities surveyed are applied to all employees in general, except for "phone call" monitoring (slightly less than one-third of all respondent companies).

	All employees in general	Specific group(s) of employees depending on job nature	**Number of companies using monitoring facilities in the area**
	% to companies using monitoring facilities in specific area		
Internet	88%	12%	**49**
Intranet/ server/ computer files	87%	11%	**47**
Email	90%	8%	**48**
Phone call	32%	64%	**25**
CCTV/Video	70%	30%	**37**
Staff card	85%	15%	**52**
Others (fingerprint electronic record, Handkey system)	50%	50%	**2**

(11) INFORMATION COLLECTED/ MONITORED AND IN WHAT MANNER

Over half to two-thirds of companies indicated that "Content" will be collected during the monitoring of "Phone calls", "Email", and "CCTV/ Video", while "Website address" or "Location" are usually captured during "Internet" and "Intranet" monitoring. Regarding the manner of collection, information collected from web/electronic devices is usually "randomly/occasionally" collected, while information from "Phone calls", "CCTV/ Video" and "Staff cards" is usually collected "continuously".

	Information collected				The information is collected/ monitored				**Number of companies using monitoring facilities in the area**
	The content	Website address/ telephone or fax number/ location	Duration/ Frequency of use/ occurrence	Others	Randomly/ occasionally	Periodically	Continuously	Collected/ monitored with a cause	
	% to companies using monitoring facilities in specific area								
Internet	27%	**73%**	43%	6%	**41%**	16%	18%	27%	**49**
Intranet/ server/ computer files	45%	**53%**	32%	6%	**36%**	13%	19%	32%	**47**
Email	**60%**	42%	23%	10%	**35%**	15%	19%	**35%**	**48**
Phone call	**56%**	28%	44%	0%	20%	4%	**64%**	8%	**25**
CCTV/Video	**76%**	22%	14%	0%	3%	5%	**73%**	19%	**37**
Staff card	31%	4%	**56%**	19%	10%	10%	**62%**	23%	**52**
Others (fingerprint electronic record, Handkey system)	0%	0%	**100%**	0%	0%	0%	**100%**	0%	**2**

(12) CONDITION FOR INFORMATION COLLECTED UNDER MONITORING BE INVESTIGATED/ REVIEWED

Over half the companies surveyed reported that they would investigate or review the information collected during monitoring if there was just cause, such as investigation of a harassment complaint. For CCTV/Video devices, 27% companies adopted real-time monitoring and thus no information was stored unless the information was to be reviewed for a good reason.

	Real-time monitoring, no information stored	Periodically	Occasionally search/ review without specific cause	Search/ reviewed with a cause (e.g., investigation of a harassment complaint)	Others	**Number of companies using monitoring facilities in the area**
	% to companies using monitoring facilities in specific area					
Internet	8%	18%	31%	**53%**	2%	**49**
Intranet/ server/ computer files	9%	17%	28%	**49%**	2%	**47**
Email	8%	10%	25%	**60%**	2%	**48**
Phone call	8%	24%	16%	**60%**	0%	**25**
CCTV/Video	27%	3%	5%	**78%**	0%	**37**
Staff card	13%	35%	8%	**50%**	0%	**52**
Others (fingerprint electronic record, Handkey system)	0%	100%	0%	0%	0%	**2**

(13) HOW MONITORING OF ELECTRONIC INFORMATION/ ELECTRONIC COMMUNICATIONS SYSTEMS IS EXECUTED

As regards the monitoring of electronic communications systems, 60% of companies collected the information by accessing the information stored in electronic communications systems. About 20% of companies with monitoring devices would intercept messages in transmission during the ordinary course of business in the internet, intranet/server and email systems.

% to companies using monitoring facilities in specific area	Intercepted messages in transmission during ordinary course of business	Intercepted messages in transmission during investigation	Accessed information stored in electronic communications systems	**Number of companies using monitoring facilities in the area**
Internet	20%	8%	65%	**49**
Intranet/ server/ computer files	19%	11%	66%	**47**
Email	19%	10%	67%	**48**
Phone call	8%	4%	84%	**25**

(14) RETENTION POLICY

Less than half of the companies using "Staff cards" and monitoring electronic communications systems (internet, intranet/server and email) specified the retention period for information collected. Among those companies specifying the retention period, a higher proportion of them would delete the information automatically.

% to companies using monitoring facilities in specific area	Retention period not specified	Retention period specified			**Number of companies using monitoring facilities in the area**
		A specific time period after which information stored is deleted		Suspension of deletion process once litigation or an investigation has commenced	
		automatically	manually		
Internet	55%	22%	6%	8%	**49**
Intranet/ server/ computer files	51%	26%	6%	11%	**47**
Email	52%	23%	10%	8%	**48**
Phone call	44%	32%	16%	20%	**25**
CCTV/Video	24%	38%	35%	22%	**37**
Staff card	58%	19%	15%	10%	**52**
Others (fingerprint electronic record, Handkey system)	0%	50%	0%	50%	**2**

(15) RETENTION PERIOD

The survey indicated that the retention periods for data collected varied across different monitoring facilities, from a minimum of one week to over 7 years.

(a) Data deleted (automatically / manually)	A specific time period after which information stored is deleted							
	Automatically				Manually			
	Mode (number of companies at the specific period)	min	max	Number of companies	Mode (number of companies at the specific period)	min	max	Number of companies
Internet	3,6 months (2)	1 week	6 month	**8**	-	1 month	5 years	**3**
Intranet/ server/ computer files	3 months (2)	1 week	1 year	**9**	-	1 week	5 years	**3**
Email	3 months (3)	1 week	1 year	**8**	1 month (2)	1 month	5 years	**4**
Phone call	1 month (3)	1 week	1 year	**8**	1 year (2)	6 months	2 years	**4**
CCTV/Video	1 month (5)	1 week	3 months	**14**	1 month (5)	1 week	3 years	**12**
Staff card	2,3,6 months (2)	1 week	2 years	**9**	7 years or above (3)	2 months	at least 7 years	**6**
Others (fingerprint electronic record, Handkey system)	1 month			**1**				

(b) Data deleted (overall)	A specific time period after which information stored is deleted			
	Overall			
	mode (number of companies at the specific period)	min	max	Number of companies
Internet	3,6 months (2)	1 week	5 years	**11**
Intranet/ server/ computer files	1 month, 3 months, 1 year (2)	1 week	5 years	**12**
Email	3 months (3)	1 week	5 years	**12**
Phone call	1 year (4)	1 week	2 years	**12**
CCTV/Video	1 month (10)	1 week	3 years	**26**
Staff card	2 months, 7 years or above (3)	1 week	at least 7 years	**15**

(16) TREND IN MONITORING POLICIES

Of the 73 companies responding to the question about their policies for monitoring in the workplace, 12% replied that they were considering extending the scope of workplace monitoring by, in most cases, using "CCTV/ video" and monitoring of "Internet" and "Email" Use.

% of companies with plans to extend the scope of workplace monitoring (to total number of responses)	12%	Total number of responses	73
Area to which the scope of monitoring is to be expanded	% to total number of responses		
Internet	4%		
Intranet/ server/ computer files	0%		
Email	5%		
Phone call	1%		
CCTV/Video	5%		
Staff card	1%		
Others	0%		

(D) OTHER ALTERNATIVES/ PRECAUTIONS

(17) PRECAUTIONS / ALTERNATIVES FOR PREVENTION OF MIS-USE OF ELECTRONIC INFORMATION/ ELECTRONIC COMMUNICATIONS SYSTEMS

In addition to monitoring through reviewing and searching information collected, companies also used other measures to prevent misuse of company electronic information/ electronic communications systems. The most popular measures were in the form of clear communication to employees about company policy, e.g., making it known to staff that "electronic communications/ computers are company property and to be used for business purposes only" (92%), that "they should not download information from the Internet if trademark or copyright is in doubt" (71%), or that "fraudulent, harassing or obscene messages are prohibited from being kept on or sent over the Internet" (63%). Also, "Training in the proper use of communications systems and the internet" was also a popular measure for preventing the misuse of systems (56%).

Measures	% of companies
<u>In general</u>	
(a) Training in the proper use of communications systems and internet	56%
Employees are alerted that	
(b) Electronic communications/ computers are company property and to be used for business purposes only	92%
(c) Electronic messages are subject to review by company management at management's discretion	42%
(d) Sending out defamatory comments is not tolerated	37%
<u>Internet environment and communication systems</u>	
(e) Confidential electronic communications are clearly marked "confidential", "proprietary information", or "attorney client privilege"	37%
(f) Company's homepage on internet displays an on-screen licensing agreement which describes the conditions under which a user can circulate or copy its materials	20%
(g) A reminder of the e-mail policy is installed in the system, which will be triggered every time an individual logs into his//her email	19%
Employees are made aware that	
(h) They should not download information from the Internet if trademark or copyright is in doubt	71%
(i) Company reserves the right to audit, intercept, access and disclose all messages created, received or sent over the electronic mail system	66%
(j) Fraudulent, harassing or obscene messages are prohibited from being kept on or sent over the Internet	63%
(k) Offensive or disruptive messages (e.g., discriminating in nature) over computerized communication systems will not be tolerated, are violation of company policy and will result in disciplinary action	53%
(l) Electronic mail system should not be used to send (upload) or receive (download) copy righted materials, trade secrets, proprietary financial information, or similar materials without prior authorization	51%
(m) Email and voicemail communications are automatically stored on a computerized backup system	44%
(n) Others	2%
Total number of companies	**86**

(E) OPINIONS OF WORKPLACE MONITORING AND EFFECTIVENESS

(18) OPINIONS OF WORKPLACE MONITORING

As a whole, most of the companies surveyed (64%) considered workplace surveillance as privacy intrusive; but only 17% reported that their companies' employee relations were adversely affected by workplace monitoring. Regarding the effectiveness of monitoring, 61% of companies considered that the use of surveillance measures had totally or to a large extent met the objectives of monitoring effectively; and 42% of companies considered that their companies had totally or to a large extent benefited from workplace surveillance. Overall, 67% of companies considered that improper behaviour and misuse of company resources in their companies were not severe.

The findings also indicated that the more companies used other communication measures, the greater the apparent effectiveness of the monitoring measures, the lesser extent to which ER is affected, the greater the extent that companies have benefited from monitoring policies, and the lesser extent to which improper behaviour and misuse of company resources were recorded.

	Totally	To large extent	To some extent	To little extent	Totally not	Don't know
	% to companies that implement workplace monitoring measures					
(a) My company considers that workplace surveillance is privacy intrusive	8%	14%	42%	13%	18%	6%
(b) My company employee relations are adversely affected by workplace monitoring (e.g., grievance or complaints raised by employees)	1%	3%	13%	28%	53%	3%
(c) The use of surveillance measures effectively meets the objectives of monitoring	11%	50%	29%	6%	0%	4%
(d) Improper behaviour and misuse of company resources in my company are not severe	22%	44%	18%	3%	10%	3%
(e) As a whole, my company has benefited from workplace surveillance	10%	32%	42%	3%	0%	14%
Total number of companies	**72**					